

539, 128

10/539128

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION  
EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété  
Intellectuelle  
Bureau international



(43) Date de la publication internationale  
15 juillet 2004 (15.07.2004)

PCT

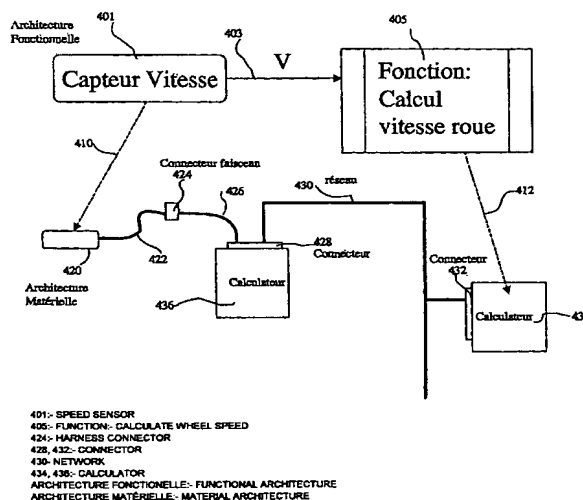
(10) Numéro de publication internationale  
WO 2004/059407 A1

- (51) Classification internationale des brevets<sup>7</sup> : G05B 23/02
- (21) Numéro de la demande internationale : PCT/FR2003/003851
- (22) Date de dépôt international : 19 décembre 2003 (19.12.2003)
- (25) Langue de dépôt : français
- (26) Langue de publication : français
- (30) Données relatives à la priorité : 02/16353 20 décembre 2002 (20.12.2002) FR
- (71) Déposant (pour tous les États désignés sauf US) : RE-NAULT s.a.s. [FR/FR]; 13-15, quai Alphonse Le Gallo, F-92100 Boulogne Billancourt (FR).
- (72) Inventeur; et
- (75) Inventeur/Déposant (pour US seulement) : BOUTIN, Samuel [FR/FR]; 10, chemin de la Chapelle, F-78114 Magny les Hameaux (FR).
- (74) Mandataire : DAVIES, Owen; Renault Technocentre, Scc 0267 TCR GRA 155, 1, avenue du Golf, F-78288 Guyancourt (FR).
- (81) États désignés (national) : JP, KR, US.
- (84) États désignés (régional) : brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR).
- Publiée :  
— avec rapport de recherche internationale

[Suite sur la page suivante]

(54) Title: METHOD FOR DIAGNOSIS OF FUNCTIONAL FAULTS IN A FUNCTIONAL ARCHITECTURE

(54) Titre : PROCÉDE DE DIAGNOSTIC DE DÉFAUTS DE FONCTIONNEMENT D'UNE ARCHITECTURE FONCTIONNELLE



(57) Abstract: The invention relates to a method for diagnosis of functional faults in a functional architecture, comprising a unit of functions connected to electronic components ( $A^n$ ;  $C^n$ ;  $UCE_n$ ; B), producing and using data, at least one datum of which ( $x_i$ ) can adopt a fixed pre-determined value ( $x_{ip}$ ), following the occurrence of an erroneous functioning of at least one of the components ( $A^n$ ;  $C^n$ ;  $UCE_n$ ; B) of said unit. The method is characterised, whilst having a unit of functions and carrying out a function for which the input and output data can be assigned to sensors or actuators, by comprising a determination step for particular values during which the particular values corresponding to functional faults for the sensors and actuators are listed and a diagnostic step during which the functional diagnostic for said function as a function of the lists determined during the determination step is generated.

(57) Abrégé : L'invention concerne un procédé de diagnostic de défauts de fonctionnement d'une architecture fonctionnelle composée d'un ensemble de fonctions liées à des composants électroniques ( $A^n$ ;  $C^n$ ;  $UCE_n$ ; B), produisant et consommant des données, au moins une desdites données ( $x_i$ ) étant susceptible de prendre une valeur particulière ( $x_{ip}$ ) prédéterminée, consécutivement à l'apparition d'un défaut de fonctionnement de l'un au moins des composants ( $A^n$ ;  $C^n$ ;  $UCE_n$ ; B).

[Suite sur la page suivante]

WO 2004/059407 A1



— avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

---

dudit ensemble, ce procédé étant caractérisé en ce que, étant donné un ensemble de fonctions, réalisant une prestation, dont les données d'entrées et de sorties peuvent être liées à des capteurs ou des actionneurs, il comporte - une étape de détermination de valeurs particulières au cours de laquelle on liste les valeurs particulières correspondant à des défauts de fonctionnement des capteurs et des actionneurs, - une étape de diagnostic au cours de laquelle on forme le diagnostic fonctionnel de ladite prestation en fonction des listes issues des étapes de détermination.

## Procédé de diagnostic de défauts de fonctionnement d'une architecture fonctionnelle

La présente invention est relative à un procédé de  
5 diagnostic de défauts de fonctionnement d'une architecture  
fonctionnelle. Ladite architecture peut être composée d'un  
ensemble de fonctions liées à des composants électroniques  
( $A_i^n$ ;  $C_i^n$ ;  $UCE_n$ ;  $B$ ), produisant et consommant des données, au  
moins une desdites données ( $x_i$ ) étant susceptible de  
10 prendre une valeur particulière ( $x_{ip}$ ) prédéterminée,  
consécutivement à l'apparition d'un défaut de  
fonctionnement de l'un au moins des composants ( $A_i^n$ ;  
 $C_i^n$ ;  $UCE_n$ ;  $B$ ) dudit ensemble.

On connaît des ensembles de systèmes électroniques de  
15 ce type, conçus notamment pour équiper des véhicules  
automobiles. Un tel véhicule comprend couramment plusieurs  
systèmes assurant chacun l'exécution d'une prestation telle  
que la commande du moteur propulsant le véhicule, la  
gestion de la climatisation de l'habitacle, la gestion des  
20 liaisons du véhicule au sol (freinage, suspension...), la  
gestion de communications téléphoniques.

On a schématisé à la figure 1 du dessin annexé les  
composants matériels de l'ensemble de ces systèmes, par  
exemple pour véhicule. Ces composants comprennent  
25 essentiellement des unités de commande électroniques ou  
"calculateurs"  $UCE_m$ , chaque calculateur étant  
éventuellement connecté à des capteurs  $C_i^n$  et à des  
actionneurs  $A_j^m$ , tous les calculateurs étant connectés à au  
moins un même bus  $B$  pour y émettre ou recevoir des  
30 informations par exemple multiplexées, en provenance ou à  
destination des autres calculateurs connectés au bus  $B$ .

Ce multiplexage est obtenu notamment, comme cela est  
bien connu pour le bus CAN par exemple, en introduisant les  
informations en cause dans des messages matérialisés par

des trames de signaux numériques.

A titre d'exemple illustratif, le système  $S_2$  de "commande du moteur" comprend le calculateur  $UCE_2$ , plusieurs capteurs  $C^2_i$  sensibles à des grandeurs telles que  
5 le régime du moteur, à combustion interne par exemple, la pression au collecteur d'admission de ce moteur, la pression de l'air extérieur, la température de l'eau de refroidissement du moteur, celle de l'air, l'état de charge de la batterie, et plusieurs actionneurs  $A^2_j$ . Le  
10 calculateur  $UCE_2$  est dûment programmé pour exécuter plusieurs fonctions de commande du moteur telles que : la régulation de ralenti, la régulation de la richesse du mélange air/carburant, le réglage de l'avance à l'allumage de ce mélange et la recirculation des gaz d'échappement.  
15 Pour ce faire le calculateur  $UCE_2$  exploite des informations venues des capteurs  $C^2_i$  précités et élabore des signaux de commande des actionneurs  $A^2_j$  constitués par une vanne de commande d'air additionnel et une bobine d'allumage de bougie pour la fonction "régulation de ralenti", un  
20 injecteur de carburant pour la fonction "régulateur de richesse", la même bobine d'allumage pour la fonction "avance de l'allumage" et une vanne pour la fonction "recirculation de gaz d'échappement".

Les autres "prestations" évoquées ci-dessus, e.g.  
25 "climatisation de l'habitable" et "liaison avec le sol", sont exécutées par des systèmes d'architecture analogue à celle présentée ci-dessus pour la commande du moteur.

Tous ces systèmes mis en communication par un même bus B constituent un réseau multiplexé. On conçoit alors que  
30 plusieurs fonctions relevant de systèmes différents peuvent exploiter des informations issues de mêmes capteurs, par exemple, ce qui évite de coûteuses redondances dans la structure de l'ensemble des systèmes. L'utilisation d'un réseau multiplexé permet aussi de réduire de manière très  
35 importante la longueur des lignes électriques

interconnectant les différents éléments de l'ensemble. Un tel ensemble multiplexé permet aussi la mise en place de fonctions non classiques et éventuellement complexes, faisant intervenir parfois plusieurs systèmes et dites pour  
5 cette raison "transversales". A titre d'exemple illustratif et non limitatif, la perception de l'information "sac d'air (ou "airbag") déclenché", significative de ce que le véhicule a subi un choc, peut être traitée alors de manière à commander l'émission d'un appel au secours par un  
10 dispositif de téléphonie mobile embarqué dans le véhicule.

Un autre étape de la conception des systèmes électroniques est l'analyse de sûreté de fonctionnement qui consiste à identifier des événements redoutés tels qu'un pneu qui éclate, un défaut de fonctionnement d'un capteur  
15 essentiel sur une fonction critique, un défaut de fonctionnement d'un actionneur par exemple de freinage, afin d'améliorer la sécurité et de spécifier des modes dégradés de fonctionnement si nécessaire.

On note qu'un système sûr de fonctionnement est un  
20 système qui, d'une part diagnostique certains événements redoutés afin de mettre en œuvre des modes de fonctionnement dégradés et d'autre part est tolérant aux événements redoutés non diagnostiqués selon l'analyse de sûreté de fonctionnement.

On connaît de la demande de brevet français N° 01  
25 15819, déposée par la demanderesse et incorporée ici par référence, la notion de valeur particulière et son utilisation dans un procédé de diagnostic de défauts de fonctionnement d'un ensemble de systèmes électroniques.

30 Cependant, ce dit procédé ne s'applique qu'à un mode de réalisation donné d'une architecture fonctionnelle et ne peut pas être réutilisé pour un autre mode de réalisation.

La demanderesse a découvert que les valeurs  
particulières pouvaient être classées en catégories de  
35 telle manière que l'on puisse séparer des valeurs particulières, dites fonctionnelles, indépendantes du mode

de réalisation par une architecture matérielle et des valeurs particulières dites opérationnelles, spécifiques au mode de réalisation par des calculateurs, bus de communication, et câblage.

5 La demanderesse a aussi découvert que les différentes catégories de valeurs particulières étaient liées en ce que une valeur particulière au niveau fonctionnel entraîne la création de valeurs particulières au niveau opérationnel. De la même manière, partant d'une analyse opérationnelle,  
10 on peut déduire une analyse fonctionnelle qui pourra être ré-appliquée sur d'autres modes de réalisations.

De cette manière on répond au problème cité ci-dessus par un procédé de diagnostic de défauts de fonctionnement d'une architecture fonctionnelle composée d'un ensemble de  
15 fonctions liées à des composants électroniques ( $A_i^n$ ;  $C_i^n$ ;  $UCE_n$ ; B), produisant et consommant des données, au moins une desdites données ( $x_i$ ) étant susceptible de prendre une valeur particulière ( $x_{ip}$ ) prédéterminée, consécutivement à l'apparition d'un défaut de fonctionnement de l'un au moins  
20 des composants ( $A_i^n$ ;  $C_i^n$ ;  $UCE_n$ ; B) dudit ensemble, ce procédé étant caractérisé en ce que, étant donné un ensemble de fonctions, réalisant une prestation, dont les données d'entrées et de sorties peuvent être liées à des capteurs ou des actionneurs, il comporte :

25 - une étape de détermination de valeurs particulières au cours de laquelle on liste les valeurs particulières correspondant à des défauts de fonctionnement des capteurs et des actionneurs,

- une étape de détermination de propagation au cours  
30 de laquelle on liste les valeurs particulières permettant la propagation de l'information relative à ces défauts à travers les dites fonctions,

- une étape de diagnostic au cours de laquelle on forme le diagnostic fonctionnel de ladite prestation en  
35 fonction des listes issues des étapes de détermination et

- une étape d'enregistrement des valeurs particulières et de leur propagation sur un moyen de mémorisation pour un outil prévu pour la validation de ladite architecture.

De cette manière on définit un diagnostic fonctionnel  
5 indépendant du mode de réalisation et donc réutilisable pour plusieurs modes de réalisation des fonctions par les calculateurs et bus. Le diagnostic est conçu avant le choix d'une architecture matérielle (calculateurs et bus) pouvant l'accueillir, ce qui permet de gagner du temps dans sa  
10 conception. Il sera comprise que le terme composants électroniques couvre tous composants électroniques et électriques produisant et consommant des données.

Selon une caractéristique particulière, après l'étape de diagnostic fonctionnel, étant donné le choix d'un mode  
15 de réalisation se traduisant par

- une architecture matérielle constituée de calculateurs, réseaux, liaisons filaires et connecteurs,
- et le placement des fonctions sur  
20 ladite architecture matérielle,

on liste les valeurs particulières selon le procédé de la revendication 1 afin de déduire un diagnostic opérationnel de l'architecture électrique-électronique résultante.

De cette manière, le diagnostic pour un placement est  
25 généré, au moins en partie, automatiquement.

Selon d'autres caractéristiques, les valeurs particulières sont classifiées après placement des fonctions sur ladite architecture matérielle

Selon d'autres caractéristiques, les valeurs  
30 particulières sont classifiées après placement des fonctions sur ladite architecture matérielle parmi au moins une des classes suivantes :

- bus coupé,
- trame corrompue,
- 35 - court-circuit appliqué à un fil,

- faux contact appliqué à un connecteur de faisceaux, de capteur, d'actionneur ou de calculateur, et
- défaut d'exécution appliqué à un micro-contrôleur.

De cette manière, le diagnostic après placement est généré automatiquement par catégories et le concepteur peut ne pas spécifier le diagnostic de certaines catégories, parce qu'elles sont plus fiables par exemple, afin de réduire le coût de conception.

Notons que le fait d'écarter une seule catégorie, par exemple les court-circuits, permet implicitement de la diagnostiquer puisque si un défaut ne provient d'aucune des autres, les défauts de ladite catégorie restent les seuls candidats à l'explication d'un problème.

Selon des caractéristiques particulières étant donné un diagnostic opérationnel, pour une prestation, ayant listé les valeurs particulières fonctionnelles relevant des capteurs, actionneurs et fonctions réalisant ladite prestation, pour au moins un flot de données entre deux fonctions, ou entre un capteur et une fonction, ou entre une fonction et un actionneur, pour lequel aucune valeur particulière fonctionnelle n'est définie, si une valeur particulière opérationnelle est définie, alors on détermine automatiquement une valeur particulière fonctionnelle nouvelle pour ce flot.

De cette manière, étant donné le diagnostic du placement d'une architecture fonctionnelle, on déduit un diagnostic fonctionnel de ladite architecture fonctionnelle qui peut s'appliquer à d'autres placements.

Selon des caractéristiques particulières, on vise un procédé de diagnostic caractérisé en ce pour chaque étape de la revendication 1, on liste non seulement les valeurs particulières, mais aussi les événements redoutés non diagnostiqués et les événements redoutés non



diagnosticables pour former une analyse de sûreté de fonctionnement d'une architecture fonctionnelle.

De cette manière, l'analyse de sûreté de fonctionnement peut être réalisée, au moins en partie, avant qu'un mode de réalisation par des calculateurs et réseaux ne soit choisi.

Selon des caractéristiques particulières, on vise un procédé de diagnostic caractérisé en ce que, étant donné le choix d'un mode de réalisation se traduisant par

- 10 - une architecture matérielle constituée de calculateurs, réseaux, liaisons filaires et connecteurs,
- et le placement des fonctions sur ladite architecture matérielle,

15 on liste les valeurs particulières et événements redoutés selon le procédé de la revendication 5 afin de déduire une analyse de sûreté de fonctionnement fonctionnelle de l'architecture fonctionnelle résultante.

De cette manière, l'analyse de sûreté de fonctionnement peut, au moins en partie, être générée automatiquement.

Le procédé peut comprendre une étape d'analyse de la faisabilité et/ou faillibilité de fonctionnement dudit architecture et de la établissement d'une sortie indiquant ladite faisabilité et/ou faillibilité.

La présente invention fournit aussi un article de commerce comportant une mémoire lisible par un ordinateur, un programme exécutable par un ordinateur étant enregistré sur ladite mémoire pour le diagnostic de défauts de fonctionnement d'une architecture fonctionnelle, caractérisé en ce que ledit programme inclut un codage pour:

- i) déterminer et lister des valeurs particulières correspondant à des défauts de fonctionnement des capteurs et des actionneurs,

ii) déterminer et lister les valeurs particulières permettant la propagation de l'information relative à ces défauts à travers ladite architecture fonctionnelle,

iii) former le diagnostic fonctionnel de ladite  
5 prestation en fonction des listes issues des étapes (i) et (ii) et

iv) enregistrer lesdites valeurs particulières et leur propagation sur un moyen de mémorisation pour un outil prévu pour la validation de ladite architecture.

10 La présente invention fournit aussi un outil informatique programmé pour le diagnostic de défauts de fonctionnement d'une architecture fonctionnelle utilisant des étapes du procédé de la présente invention ou programmé en utilisant un article de commerce de la présente  
15 invention.

Ledit architecture peut comporter un architecture pour équiper un véhicule.

D'autres buts, caractéristiques et avantages de la présente invention apparaîtront à titre d'exemple à la  
20 lecture de la description qui va suivre et à l'examen du dessin annexé dans lequel :

- la figure 1 est un schéma d'un ensemble de systèmes électroniques qu'on se propose de doter de moyens de diagnostic de défauts de  
25 fonctionnement suivant la présente invention, cet ensemble étant décrit dans le préambule de la présente description et,

- la figure 2 est un schéma illustrant un type de placement d'une fonction sur une architecture  
30 matérielle

En figure 2, la fonction "Calcul vitesse roue" 405 consomme une donnée brute "V" 403, provenant du capteur "vitesse roue" 401. Un diagnostic de la donnée V peut être déterminé à partir d'une information provenant du capteur  
35 "vitesse roue" 401 ou par un filtrage en entrée de la fonction "Calcul vitesse roue" 405. Supposons que ce

diagnostic soit déterminé par une valeur particulière de "V" 403, par exemple la valeur particulière "Vpart" de "V".

Dans la figure 2, dans un mode de réalisation particulier, le capteur vitesse 420 est rattaché à un  
5 calculateur 436 et la fonction "Calcul vitesse roue" 405 est réalisée par un processus exécuté sur un autre calculateur 434.

La transformation du capteur vitesse 401 d'une architecture fonctionnelle en capteur vitesse 420 d'une  
10 architecture matérielle est symbolisé par la flèche 410. De même, l'implantation de la fonction "Calcul vitesse roue" 405 de l'architecture fonctionnelle sur le calculateur 434 est symbolisé par la transformation 412. On note que le flot de données entre le capteur vitesse 401 et la fonction  
15 "Calcul vitesse roue" 405 est transformé en un chemin complexe de l'architecture matérielle, chemin impliquant :  
- deux calculateurs 436 et 434 et leur connecteurs respectifs 428 et 432,  
- un réseau 430,  
20 - des liaisons filaires 422 et 426, et  
- un connecteur de faisceaux 424.

Une valeur particulière A de type "court circuit" est associée au chemin formé des fils 422 et 426 entre le capteur 420 et le calculateur 436 auquel il est rattaché,  
25 cette valeur caractérisant aussi un défaut de connexion au niveau de l'un, au moins, des connecteurs 424 et 428.

Une valeur particulière B caractérisant l'état de fonctionnement du calculateur 436 indique si le relai de la donnée "V" sur ce dit calculateur 436 peut s'effectuer dans  
30 de bonnes conditions.

Une valeur particulière C caractérisant l'état de fonctionnement du bus 430 prend en compte l'absence de transmission de la donnée "V" sur ledit bus 430.

Les valeurs particulière A, B, C sont, conformément à  
35 l'invention, considérées en plus de la valeur particulière de V pour le diagnostic du flot de données entre le capteur de vitesse 420 et l'exécution de la fonction "Calcul vitesse roue" sur le calculateur 434 sur lequel elle est

placée.

Les valeurs particulière A, B, C qui peuvent être des valeurs particulières de "V" ou d'une ou plusieurs autres données, peuvent être déterminés automatiquement à partir  
5 de la projection du flot de données sur l'architecture matérielle.

En effet,

- les types de défauts entre un capteur et un calculateur ou entre un calculateur et un actionneur sont des  
10 défauts de connectique sur le chemin filaire suivi par la donnée V et peuvent être caractérisés par une valeur particulière sur le calculateur recevant le signal à condition qu'il existe une fonction pour les diagnostiquer;
- 15 - les types de défauts liés à l'exécution d'une fonction sur un calculateur sont diagnostiqués par ledit calculateur, un mode de réalisation étant l'émission d'une valeur particulière en cas d'échec d'un calcul de CRC (Cyclic Redundancy Check) ou test de redondance  
20 cyclique par exemple ou encore l'émission systématique d'une valeur particulière signalant le bon fonctionnement du calculateur, la valeur particulière ayant alors le rôle d'un diagnostic de bon fonctionnement et l'absence d'émission de ladite valeur  
25 particulière correspondant alors à un défaut de fonctionnement dudit calculateur; et
- les types de défauts liés à la transmission de données sur un bus sont générés à partir d'une stratégie de gestion de réseau où chaque calculateur du réseau  
30 observe les autres et interprète une absence de réception comme une perte transitoire de connexion, ceci pouvant être caractérisé par une valeur particulière.

Dès lors, pendant l'étape de placement, le diagnostic de la donnée V peut être enrichi des valeurs particulières  
35 A, B et C, afin d'aider à la localisation d'un éventuel défaut, en plus de la valeur particulière "Vpart" provenant du capteur déjà spécifié avant placement dans l'architecture fonctionnelle.

Réciproquement, étant donné un diagnostic pour le mode de réalisation de la figure 2, si une valeur particulière est définie pour l'un quelconque des éléments 420, 422, 424, 426, 428, 436, 430 et 432, pour la consommation de la donnée V par la fonction "Calcul vitesse roue", alors on peut en déduire qu'il est nécessaire de spécifier au moins une valeur particulière du flot de données V dans l'architecture fonctionnelle.

On note que le procédé ainsi définit s'étend sans peine à un procédé d'analyse de sûreté de fonctionnement, l'analyse de sûreté de fonctionnement pratiquée sur une architecture fonctionnelle pouvant ensuite être raffinée au moment du placement de ladite architecture fonctionnelle sur une architecture matérielle. Le seul enrichissement réside en ce que dans une analyse de sûreté de fonctionnement, on considère non seulement des valeurs particulières correspondant à des défauts détectables par le système, mais on prend aussi en compte des événements redoutés non détectés par le système.

Cependant, ce changement de point de vue ne modifie pas le procédé proposé dans la présente invention.

Ci-dessous, on prend l'exemple de la prestation accès à un véhicule et on s'intéresse plus particulièrement à la sûreté de fonctionnement de la prestation en cas de "CRASH", c'est-à-dire d'accident grave détecté par un capteur spécifique, ici un accéléromètre. Dans un tel contexte, le cas d'utilisation que nous appellerons "CRASH" est: "Dans un contexte moteur tournant, si un crash est détecté, alors les ouvrants du véhicule doivent se déverrouiller d'urgence". On veut s'assurer qu'effectivement, suite à un crash, les portes seront déverrouillées afin que les sauveteurs puissent enlever rapidement les passagers du véhicule, par exemple. Tous les événements qui peuvent nuire à la bonne exécution de ce cas d'utilisation sont redoutés.

Dans la suite, on appelle pilote une fonction dédiée à la gestion d'un capteur ou d'un actionneur, c'est à dire la fonction de capture et mise en forme d'une donnée

provenant d'un actionneur ou la fonction de mise en forme d'une donnée de consigne et commande d'un actionneur suivant ladite consigne.

Pour implémenter le cas du CRASH, une requête "crash  
5 détecté" est spécifiée. Elle est réalisée par une fonction  
appelée "crash-détecté" qui capture la valeur fournie par  
un accéléromètre "A". Cette valeur est évaluée en un bit de  
statut "a" indiquant si un choc est détecté. Le pilote  
logiciel de capture de l'accélération en provenance du  
10 capteur "A" est le programme "P1". lorsqu'un Crash est  
détecté, le système pas dans un état que nous nommerons  
"Déverrouillage d'urgence". Dans cet état, la fonction  
"déverrouillage des portes" est exécutée. Cette exécution  
résulte en l'affectation d'une donnée "d" à la valeur "1"  
15 lue par un pilote (programme de commande d'actionneur des  
verrous) logiciel P2 qui commande à l'ouverture les verrous  
des portes Vi.

Le séquençement des opérations en cas de crash est  
alors par exemple:

- 20 - l'accéléromètre a détecté une valeur de crash,
- le pilote P1 est exécuté,
- la fonction qui réalise la demande "crash  
détecté" est évaluée,
- le bit "a" de détection du crash est mis à la  
25 valeur "1", ce qui correspond dans notre exemple à  
une validation du passage dans l'état suivant :
  - le passage dans l'état "Déverrouillage  
d'urgence" est réalisé,
  - l'opération élémentaire déverrouillage des  
30 portes est activée,
  - la donnée "d" est mise à la valeur "1",
  - le logiciel P2 est exécuté, et
  - les verrous Vi sont commandés en position  
déverrouillé.

35 Si on s'intéresse aux événements redoutés qui  
affectent l'opération élémentaire crash-détecté-valide, on  
a par exemple :

- le capteur A est défaillant, et

- P1 est défaillant,

On suppose que, pour chacune de ces défaillances, si elles peuvent être diagnostiquées, les fonctions passent éventuellement dans un mode de fonctionnement dégradé  
5 suivant un procédé connu. Dans le procédé que nous présentons, la notion de passage en mode dégradé, bien connue de l'homme du métier, n'intervient pas, le passage au niveau fonctionnel et au niveau opérationnel étant équivalent. Nous ne parlerons donc pas de cet aspect de  
10 l'analyse de sûreté de fonctionnement dans notre description.

Si, maintenant, l'opération élémentaire crash-detecté-valide est placée sur un calculateur UCH et si, d'une part, le capteur A est attaché à un calculateur "Airbag", et,  
15 d'autre part, ces deux calculateurs sont liés par un bus de donnée CAN et que la donnée A circule sur la trame T, alors les événements redoutés qui affectent l'opération élémentaire sont enrichis et deviennent :

- le capteur A est intrinsèquement défaillant,
- 20 - l'un des fils ou des connecteurs entre le capteur A et le calculateur Airbag est en défaut (fil coupé, défaut de connectique,...),
- l'un des autres fils et connecteurs liant le capteur A aux autres calculateurs est en défaut et  
25 crée un défaut du capteur A,
- l'exécution de P1 est défaillante,
- le calculateur Airbag sur lequel P1 s'exécute est en défaut,
- le bus CAN est coupé,
- 30 - la trame T ne circule pas suite à un défaut du pilote CAN sur l'Airbag,
- la trame T n'est pas lue correctement par le calculateur habitacle, et
- le calculateur habitacle est en défaut.

35 Suivant un autre placement, d'autres événements correspondant aux nouveaux calculateurs et réseaux et éléments de connectique impliqués sont spécifiés.

On peut donc, lors de la description de la prestation,

spécifier un ensemble d'événements s'appliquant aux capteurs, actionneurs, pilotes, données, opérations élémentaires. Lorsque le placement est réalisé, le placement sur des calculateurs connectés par des réseaux permet d'enrichir automatiquement la description des passages en modes dégradés ou des propagations de défaut en prenant en compte :

- pour un capteur ou un actionneur, l'ensemble des défauts pour chaque fil, et chaque connecteur liant ce capteur ou cet actionneur aux différents calculateurs et masses,
- pour un pilote, un défaut d'exécution logiciel ou un défaut de la plate-forme sur laquelle il est placé,
- pour une donnée si elle circule sur un réseau, une coupure du réseau,
- pour une donnée si elle circule dans une trame, un défaut de la trame,
- pour une donnée si elle circule sur un calculateur passerelle entre deux réseaux, un défaut du calculateur, et
- pour une opération élémentaire, un défaut d'exécution logiciel ou un défaut du calculateur sur lequel est placé l'opération élémentaire.

L'ensemble des types de défaut ainsi que les composants auxquels ces types de défaut peuvent s'appliquer sont renseignés dans une base de donnée. Les enrichissements des événements suite au placement sont ainsi réalisés automatiquement.

Ce procédé peut être mis en œuvre à l'aide d'un outil informatique permettant l'édition des différents objets nécessaires à la conception et l'automatisation partielle des différentes étapes du procédé constitué par l'invention.

Le procédé peut comprendre une étape d'analyse de la faisabilité et/ou faillibilité de fonctionnement dudit architecture et de la établissement d'une sortie indiquant ladite faisabilité et/ou faillibilité. L'architecture peut



comporter un architecture pour équiper un véhicule, par exemple une voiture ou une camionnette.

5 Le procédé de l'invention peut être programmé sur un article de commerce comportant une mémoire lisible par un ordinateur, par exemple un CD, DVD ou équivalent ou sur le disque dur d'un ordinateur. Un tel programme pour le procédé sera exécutable par un ordinateur, et sera enregistré sur ladite mémoire pour être exécuté par ledit ordinateur.

REVENDICATIONS

1. Procédé de diagnostic de défauts de fonctionnement d'une architecture fonctionnelle composée d'un ensemble de fonctions liées à des composants électroniques ( $A_i^n$ ;  $C_i^n$ ;  $UCE_n$ ;  $B$ ), produisant et consommant des données, au moins une desdites données ( $x_i$ ) étant susceptible de prendre une valeur particulière ( $x_{ip}$ ) prédéterminée, consécutivement à l'apparition d'un défaut de fonctionnement de l'un au moins des composants ( $A_i^n$ ;  $C_i^n$ ;  $UCE_n$ ;  $B$ ) dudit ensemble, ce procédé étant caractérisé en ce que, étant donné un ensemble de fonctions, réalisant une prestation, dont les données d'entrées et de sorties peuvent être liées à des capteurs ou des actionneurs, il comporte :
- 15 i) une étape de détermination de valeurs particulières au cours de laquelle on liste les valeurs particulières correspondant à des défauts de fonctionnement des capteurs et des actionneurs,
  - 20 ii) une étape de détermination de propagation au cours de laquelle on liste les valeurs particulières permettant la propagation de l'information relative à ces défauts à travers les dites fonctions,
  - 25 iii) une étape de diagnostic au cours de laquelle on forme le diagnostic fonctionnel de ladite prestation en fonction des listes issues des étapes de détermination, et
  - 30 iv) une étape d'enregistrement des valeurs particulières et de leur propagation sur un moyen de mémorisation pour un outil prévu pour la validation de ladite architecture.
2. Procédé de diagnostic selon la revendication 1, caractérisé en ce qu'après l'étape (iii) de diagnostic fonctionnel, étant donné le choix d'un mode de réalisation se traduisant par
- 35 - une architecture matérielle constituée de

calculateurs, réseaux, liaisons filaires et connecteurs, et

- le placement des fonctions sur ladite architecture matérielle.

5        on liste les valeurs particulières selon le procédé de la revendication 1 afin de déduire un diagnostic opérationnel de l'architecture électronique résultante.

3. Procédé de diagnostic selon les revendications 1 ou  
10 2, caractérisé en ce que les valeurs particulières sont classifiées après placement des fonctions sur ladite architecture matérielle.

4. Procédé de diagnostic selon la revendication 3,  
15 caractérisé en ce que les valeurs particulières sont classifiées parmi au moins une des classes supplémentaires suivantes :

- bus coupé,
- trame corrompue,
- 20 - court-circuit appliqué à un fil,
- faux contact appliqué à un connecteur de toron, de capteur, d'actionneur ou de calculateur, et
- défaut d'exécution appliqué à un micro-  
25 contrôleur.

5. Procédé selon les revendications 1 à 4, caractérisé en ce que étant donné un diagnostic opérationnel, pour une prestation, ayant listé les valeurs particulières  
30 fonctionnelles relevant des capteurs, actionneurs et fonctions réalisant ladite prestation, pour au moins un flot de données entre deux fonctions, ou entre un capteur et une fonction, ou entre une fonction et un actionneur, pour lequel aucune valeur particulière fonctionnelle n'est  
35 définie, si une valeur particulière opérationnelle est

définie, alors on détermine automatiquement une valeur particulière fonctionnelle nouvelle pour ce flot.

5 6. Procédé selon les revendications 1 à 5, caractérisé en ce que on liste les événements redoutés non diagnostiqués et les événements redoutés non diagnosticables pour former une analyse de sûreté de fonctionnement d'une architecture fonctionnelle.

10 7 Procédé selon les revendications 1 à 6, caractérisé en ce que, étant donné le choix d'un mode de réalisation se traduisant par

- une architecture matérielle constituée de calculateurs, réseaux, liaisons filaires et connecteurs,
- 15 - et le placement des fonctions sur ladite architecture matérielle,

on liste les valeurs particulières et événements redoutés selon le procédé de la revendication 6 afin de déduire une  
20 analyse de sûreté de fonctionnement fonctionnelle de l'architecture fonctionnelle résultante.

8. Procédé de diagnostic selon l'une quelconque des revendications 1 à 7, caractérisé en ce que ledit  
25 architecture comporte un architecture pour équiper un véhicule.

9. Procédé de diagnostic selon l'une quelconque des revendications 1 à 8, caractérisé en ce qu'il comprend une  
30 étape d'analyse de la faisabilité et/ou faillibilité de fonctionnement dudit architecture et de la établissement d'une sortie indiquant ladite faisabilité et/ou faillibilité.

10. Un article de commerce comportant une mémoire lisible par un ordinateur, un programme exécutable par un ordinateur étant enregistré sur ladite mémoire pour le diagnostic de défauts de fonctionnement d'une architecture fonctionnelle, caractérisé en ce que ledit programme inclut  
5 un codage pour:

- i) déterminer et lister des valeurs particulières correspondant à des défauts de fonctionnement des capteurs et des actionneurs,
- 10 ii) déterminer et lister les valeurs particulières permettant la propagation de l'information relative à ces défauts à travers ladite architecture fonctionnelle,
- iii) former le diagnostic fonctionnel de ladite prestation en fonction des listes issues des étapes (i) et  
15 (ii) et
- iv) enregistrer lesdites valeurs particulières et leur propagation sur un moyen de mémorisation pour un outil prévu pour la validation de ladite architecture.

20 11. Un outil informatique programmé pour le diagnostic de défauts de fonctionnement d'une architecture fonctionnelle utilisant des étapes du procédé selon l'une quelconque des revendications 1 à 9 ou programmé en utilisant un article de commerce selon la revendication 10.

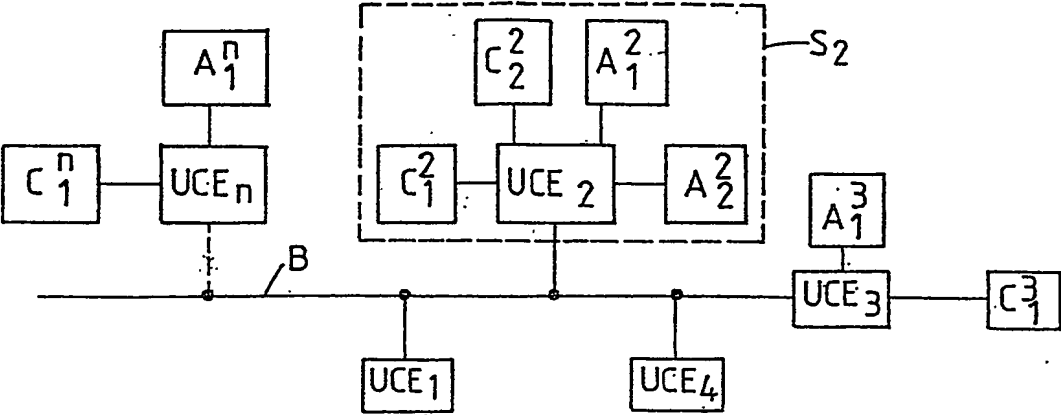


FIG.:1 (TECHNIQUE ANTERIEURE)

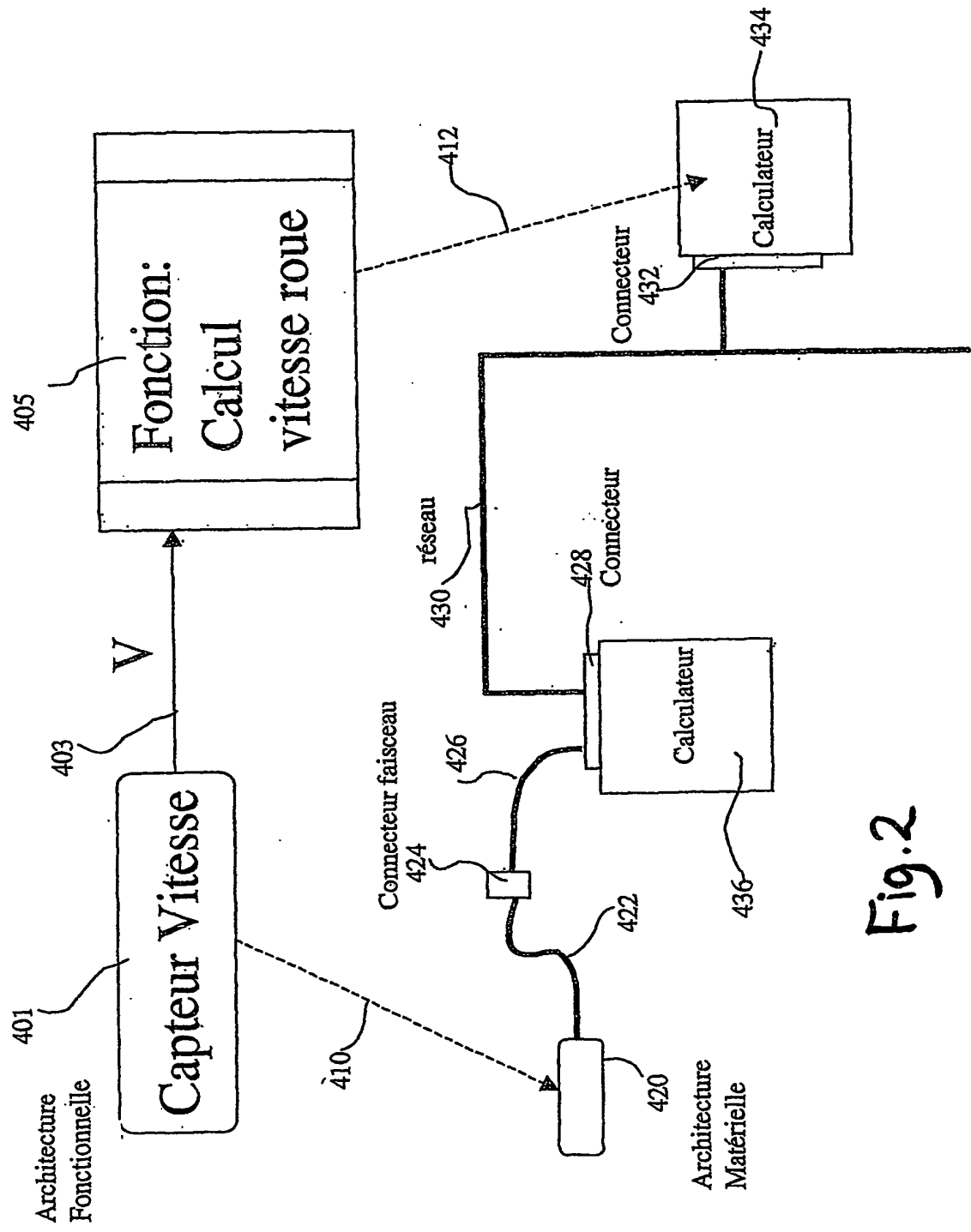


Fig.2

# INTERNATIONAL SEARCH REPORT

PCT/FR 03/03851

## A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 G05B23/02

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 G05B G05D B60K B60L B60R G07C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EP0-Internal

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 02/071360 A (TUSZYNSKI JAN ; GOALART AB (SE); OEHRMAN BENGT (SE); DAHLSTRAND FREDRIK) 12 September 2002 (2002-09-12)	1, 10, 11
Y	page 8, line 23 - page 14, line 10; claim 1	8
Y	US 5 939 625 A (TORII KENJI ET AL) 17 August 1999 (1999-08-17) figure 4	8
P, A	FR 2 833 353 A (RENAULT) 13 June 2003 (2003-06-13) cited in the application page 4, line 1 - page 9, line 4; claim 1	1, 8
A	EP 0 707 250 A (OMRON TATEISI ELECTRONICS CO) 17 April 1996 (1996-04-17) column 16, line 33 - column 22, line 28	1
	-/-	

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

### \* Special categories of cited documents:

- \*A\* document defining the general state of the art which is not considered to be of particular relevance
- \*E\* earlier document but published on or after the international filing date
- \*L\* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- \*O\* document referring to an oral disclosure, use, exhibition or other means
- \*P\* document published prior to the international filing date but later than the priority date claimed

- \*T\* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- \*X\* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- \*Y\* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- \*G\* document member of the same patent family

Date of the actual completion of the international search

10 June 2004

Date of mailing of the international search report

17/06/2004

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Authorized officer

Kelperis, K



# INTERNATIONAL SEARCH REPORT

PCT/FR 03/03851

## C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>DE 100 48 144 A (WILHELM UWE ; DOHMANN  AXEL (DE)) 18 April 2002 (2002-04-18)  claim 1</p> <p>-----</p>	

# INTERNATIONAL SEARCH REPORT

Information on patent family members

PCT/FR 03/03851

Patent document cited in search report		Publication date		Patent family member(s)	Publication date
WO 02071360	A	12-09-2002	SE	522545 C2	17-02-2004
			EP	1377949 A1	07-01-2004
			EP	1377950 A1	07-01-2004
			SE	522549 C2	17-02-2004
			SE	0101525 A	07-09-2002
			SE	0101526 A	07-09-2002
			WO	02071359 A1	12-09-2002
			WO	02071360 A1	12-09-2002
US 5939625	A	17-08-1999	JP	3481046 B2	22-12-2003
			JP	9330119 A	22-12-1997
FR 2833353	A	13-06-2003	FR	2833353 A1	13-06-2003
			WO	03048878 A1	12-06-2003
EP 0707250	A	17-04-1996	EP	0707250 A1	17-04-1996
			US	5742624 A	21-04-1998
			WO	9404969 A1	03-03-1994
			JP	2687726 B2	08-12-1997
DE 10048144	A	18-04-2002	DE	10048144 A1	18-04-2002

# RAPPORT DE RECHERCHE INTERNATIONALE

PCT/FR 03/03851

**A. CLASSEMENT DE L'OBJET DE LA DEMANDE**  
CIB 7 G05B23/02

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

**B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE**

Documentation minimale consultée (système de classification suivi des symboles de classement)

CIB 7 G05B G05D B60K B60L B60R G07C

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

EPO-Internal

**C. DOCUMENTS CONSIDERES COMME PERTINENTS**

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	WO 02/071360 A (TUSZYNSKI JAN ; GOALART AB (SE); OEHRMAN BENGT (SE); DAHLSTRAND FREDRIK) 12 septembre 2002 (2002-09-12)	1, 10, 11
Y	page 8, ligne 23 - page 14, ligne 10; revendication 1	8
Y	US 5 939 625 A (TORII KENJI ET AL) 17 août 1999 (1999-08-17)	8
	figure 4	
P, A	FR 2 833 353 A (RENAULT) 13 juin 2003 (2003-06-13)	1, 8
	cité dans la demande	
	page 4, ligne 1 - page 9, ligne 4; revendication 1	
	----- -/-	

☒ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

\* Catégories spéciales de documents cités:

- \*A\* document définissant l'état général de la technique, non considéré comme particulièrement pertinent
- \*E\* document antérieur, mais publié à la date de dépôt international ou après cette date
- \*L\* document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
- \*O\* document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
- \*P\* document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

- \*T\* document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
- \*X\* document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
- \*Y\* document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
- \*Z\* document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

10 juin 2004

Date d'expédition du présent rapport de recherche internationale

17/06/2004

Nom et adresse postale de l'administration chargée de la recherche internationale  
Office Européen des Brevets, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax (+31-70) 340-3016

Fonctionnaire autorisé

Kelperis, K

# RAPPORT DE RECHERCHE INTERNATIONALE

PCT/FR 03/03851

## C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	EP 0 707 250 A (OMRON TATEISI ELECTRONICS CO) 17 avril 1996 (1996-04-17) colonne 16, ligne 33 - colonne 22, ligne 28 -----	1
A	DE 100 48 144 A (WILHELM UWE ; DOHMANN AXEL (DE)) 18 avril 2002 (2002-04-18) revendication 1 -----	

# RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

PCT/FR 03/03851

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 02071360	A	12-09-2002	SE 522545 C2	17-02-2004
			EP 1377949 A1	07-01-2004
			EP 1377950 A1	07-01-2004
			SE 522549 C2	17-02-2004
			SE 0101525 A	07-09-2002
			SE 0101526 A	07-09-2002
			WO 02071359 A1	12-09-2002
			WO 02071360 A1	12-09-2002
US 5939625	A	17-08-1999	JP 3481046 B2	22-12-2003
			JP 9330119 A	22-12-1997
FR 2833353	A	13-06-2003	FR 2833353 A1	13-06-2003
			WO 03048878 A1	12-06-2003
EP 0707250	A	17-04-1996	EP 0707250 A1	17-04-1996
			US 5742624 A	21-04-1998
			WO 9404969 A1	03-03-1994
			JP 2687726 B2	08-12-1997
DE 10048144	A	18-04-2002	DE 10048144 A1	18-04-2002